TELKOMNIKA, Vol.17, No.3, June 2019, pp.1324~1337
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v17i3.10050

Risk assessment of information production using extended risk matrix approach

Jaka Sembiring*, Fitasari Wiharni
School of Electrical Engineering and Informatics, Institut Teknologi Bandung, Indonesia
*Corresponding author, e-mail: jaka@itb.ac.id

Abstract

In many cases poor information quality appears mainly due to in-effectiveness of information management including information production and delivery. Where this situation poses a certain risk. A holistic information risk management model has been previously proposed. But the model has some limitations especially on risk calculation and risk priority ranking as the model does not consider existing control effectiveness. In this paper, a new risk assessment method is proposed in order to improve the model of total impact of risks and to improve the accuracy of risk priority ranking by modifying the extended risk matrix approach (RMA) where we take into account the existing control effectiveness. Using our approach by adding a new dimension on extended RMA. We are able to improve the accuracy (7.15%) and reduced the ambiguity (1.34) of assessment results on real cases illustration.

Keywords*: information production, information quality, risk assessment, risk matrix*

1. Introduction

It is widely understood that information is a strategic asset for an enterprise so that it has to be maintained. This fact is especially true for organization whose information production is their main activity [1]. Moreover. information proliferation has increased the global sales of business intelligence and analytics software at around 22% in 2008 [2]. But when delivery of data and information assets is not aligned with its objectives and intended goals then problems of information quality (IQ) will arise. This problem could be the source of various losses, big risks and even catastrophe especially when it leads to an incorrect decision making [3, 4].

An information system is required to ensure information quality which is valuable in decision making [5, 6]. In-effective information management including information production and delivery leads to a poor information quality and creates a negative risk impact [7]. Failure of obtaining expected information quality is the most influential aspect if not the main cause of various risks or losses [8]. In this case, risk management has an important role to protect information assets through systematically and holistically manage information quality [3]. One of important part of risk management is risk assessment process where it provides a process sequence. Allocates resource to mitigate risk, and issues an alarm as a warning to handle the risk [9, 10]. Through understanding of information quality risk assessment. Organization is equipped with a tool to realize the priority areas to improve information quality.

Total Information Risk Management (TIRM) (2013) is a concept, method, technique and approach for risk management in information quality context. This model provides a systematically risk assessment framework to calculate total impact of risk for some business objectives such as financial, customer satisfaction, compliance and so on. This model also integrates many techniques in risk assessment area especially for priority ranking of information risks such as fault-tree analysis, bow-tie, risk matrix etc. Priority ranking using risk matrix approach employs two dimensions that is considered effective for decision making in risk management context [11]. Upon examination there seems to be some drawbacks in this model, since existing control effectiveness is out of consideration. The impact and likelihood are obtained by estimating the influence of existing control without considering its effectiveness of the control so that the residual impact and likelihood cannot be determined accurately. Furthermore, Risk matrix approach only considers two dimensions i.e. severity and frequency. If we take into account this existing control then there is a possibility to improve the matrix for a better decision making.

Received May 28, 2018; Revised February 5, 2019; Accepted March 3, 2019

In this paper, we propose an information production risk assessment procedure by deriving a new calculation method for total impact in financial objectives. We employ the threat dependency scenario model as a building block to obtain total impact while at the same time consider the control effectiveness that has been implemented. In addition we propose a new method to increase accuracy of risks priority ranking when we take into account the effectiveness of existing control. We adopt the ISO 27005:2008 standard framework where risk assessment processes include asset, threat, control and vulnerability as risk factors. Considering existing control, we propose recoverability as an addition dimension to risk matrix approach derived in [10] to improve its function. Finally we provide a real case implementation of our proposed method in a government institution. In this paper, section 2 describes related works, section 3 describes our proposed method, and a real case illustration will be elaborated in section 4, and finally we conclude our study in section 5.

2. Related Works

As mentioned before, TIRM provides a holistic and systematic information risk management. This model is based on ISO 31000 standard and provides mathematical model to calculate total impact through frequency of a task. A probability of required information, frequency of information quality problem, and probability of direct and indirect impact [7]. On the model, examination of existing risk control is a very important step to identify whether existing controls already been implemented to prevent IQ problem and/or their consequences [7]. Without understanding what kind of control which is applied as respond to a risk, error will arise in risk analysis and evaluation [3]. To assess existing risk control, one has to understand how effective is the control that has been applied in the organization. In this context, there seems to be some limitation on the TIRM model. It does not include existing control effectiveness explicitly to calculate total impact. The model only identifies what existing control is, and it estimate likelihood and impact without modelling the probability of control effectiveness. As a consequence there is no guarantee that the result will produce exactly how effective existing control is, what the likelihood is, and how big the residual impact is. These facts may cause errors in risk analysis result.

In other development, Risk Matrix Approach (RMA) is a technique used in risk assessment, especially for risk priority ranking proposed by Electronic System Centre. This technique has been widely used in industry [7, 11]. This approach has been integrated into the TIRM model at risk evaluation and ranking stage [7]. In RMA, risk matrices consists of two key matrix which is impact and likelihood of risk. This technique is useful for qualitatively identifying which risks are the most critical and has enabled industry to determine the priority for corrective action [10, 11]. In addition, the risk matrix is also an effective tool and widely used to improve risk management decisions [11]. Nevertheless, it appears that some disadvantages of this technique exist. The index classification is less accurate, assessment mechanisms are based on subjective calculation and the matrix has not always been able to meet the needs and complexity of risk assessment diversities [10]. Moreover this technique is not as simple as it is claimed to be. It takes a lot of considerations and requirements to create an ideal matrix to improve risk management decisions, since it is based only on aggregation or merging of two attributes, namely the likelihood and impact [11].

To overcome those weakness, there has been already several attempts to improve applicability of risk matrix approach, such as clustering algorithm to improve risk matrix classification index [12]. Borda method is also developed to improve risk matrix precision, although this effort cannot eliminate risk ties completely [13]. There are also some proposed risk calculation algorithm to improve objectivity of assessment process [14]. All of these developments are relied on the original published risk matrix where matrix dimension is limited to two dimension and for many cases this limitation create inflexibility in risk assessment problem and requirements [10]. There are some proposed frameworks to extend the risk matrix approach. Extension framework of RMA techniques is proposed by [10] to address complexity and to meet the risk assessment requirements. The purpose of this extension is to widen its applicability where input variables can be selected from variety of options with different combinations according to requirement on actual situation [15]. Recoverability has been proposed as an additional dimension to address the complexity of risk assessment in supply chain area, where recoverability is defined as the system's ability to achieve acceptable limits or levels of operation after a risk event occurs [10].

In the previously mentioned risk assessment mathematical model and risk matrix approach, the role of existing control effectiveness has not been treated or considered. To improve the overall accuracy of the model, in this paper we will create a formulation to determine residue likelihood and impact involving existing control effectiveness. We will show that the risk assessment result is better to represent the actual conditions. We develop further a new dimension namely recoverability in the context of information quality to improver the accuracy of the extend risk matrix approach. In final section we will show the implementation of our proposed method in a real government institution.

3. Proposed Method

In this paper, our proposed information quality risk assessment method is limited to information production domain which consists of four steps**.** We utilize the dimensions in this domain to assess information quality as an input for risk assessment process. Then, we define information system components as assets to support information quality. We develop a conceptual model to map the risk factors and their relation. Based on this relation we develop probability model in a step-by-step procedure to calculate the risk assessment.

3.1. Conceptual Model

Information production as our object of research is defined as an information creation phase, which is supported by information system components where this information system is considered as assets where each asset has threats, vulnerabilities and controls. The existing control identification in this proposed model will adopt the types of control described in [16] i.e. preventive, dissuasive, protective, palliative and recuperative. Our construction of conceptual model is based on the following principles.

- The controls in use have different types, where depend on these control types one can determine the effectiveness of control to reduce likelihood and impact;
- Control is applied to a threat that exploit vulnerabilities or several vulnerabilities in relevant assets;
- Threats can exploit more than one vulnerabilities;
- A threat that successfully exploits vulnerabilities could affect more than one technical impact;
- Reductions of information quality characteristics affect the financial impact.

Based on the above principles, we create a conceptual model illustrated in Figure 1, where in general we adopt the model proposed in [16]. Conceptual model as in Figure 1 described components of the model and relationships between them. The components consists of controls, threats, vulnerabilities and both of technical and financial impact. The list of assets used in this study is described in Table 1 where we adopted [17]. Each asset can be seen in our unified conceptual model.

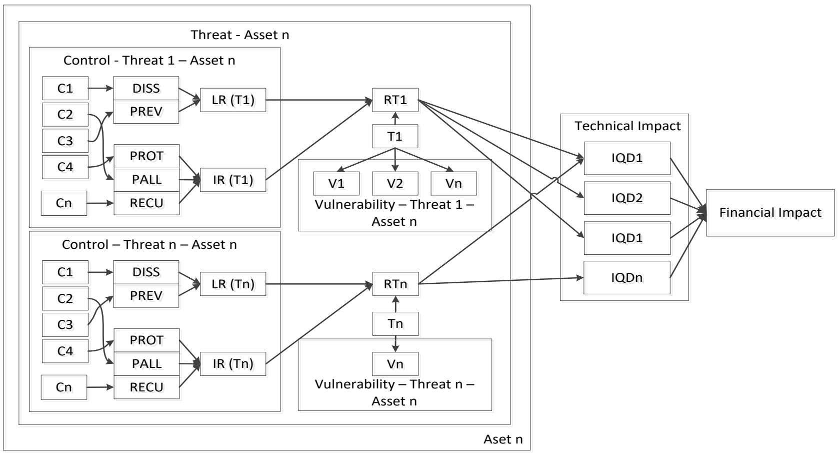

Figure 1. Proposed conceptual model

Table 1. List of Assets

Code	Asset
A1	Data and information
A2	Software
A3	Hardware
A4	Network
A5	Auxiliary equipment
A6	Physical infrastructure
A7	Personnel

Notes

Asset n	: Asset – n
IQD n	: Information quality dimension – n
Vn	: Vulnerability – n
Tn	: Threat – n
Cn	: Control – n
DISS	: Control combination effectiveness for Dissuasive
PREV	: Control combination effectiveness for Preventive
PROT	: Control combination effectiveness for Protective
PALL	: Control combination effectiveness for Palliative
RECU	: Control combination effectiveness for Recuperative
LR(Tn)	: Control combination effectiveness for likelihood reduction
IR(Tn)	: Control combination effectiveness for impact reduction

3.2. Probability Model

The detail of construction of the above conceptual model can be described step by step as follows:

Step 1: Determining scope of assessment.

In this step, we define assessment scope of business process. This scope can be defined as primary or supporting business process or based on business process criticality. Then we determine the business objective such as financial, operational efficiency, strategy, customer satisfaction etc. In this paper, we focus only on financial aspect of business objective.

Step 2: Performing information quality assessment.

Information quality assessment is conducted to get ideal (target) and existing quality. In this step we refer to the information process flow described in [18. 19] as illustrated in Figure 2. Information process consists of two phases called information production phase (source, transfer and process) and information delivery phase (access and use). Each process (source, transfer and so on) has different dimension as its information quality parameters.

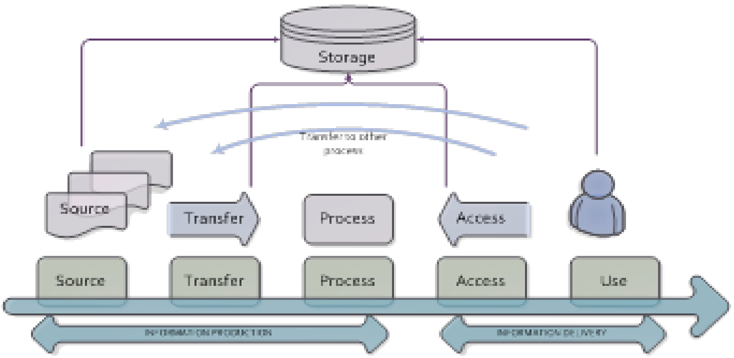

Figure 2. Information process flow [18, 19]

To determine IQ dimension standard, we create IQ dimension–attribute catalogue. This catalogue describes what attributes will be used in IQ assessment. In this paper we will focus only on information production phase risk assessment. Therefore, we will use IQ dimensions related to source, transfer and process (information production phase). There are eight dimensions for source and process, and one dimension for transfer [8]. Although, transferability dimension is rarely mentioned in literatures, we still assume that this characteristic is important. Transferability is distribution value from one process to another process and a part of information network (communication infrastructure and access to data and information) [8]. To develop IQ dimension-attribute catalogue, we refer to [20] for the summary of dimension and attribute comparison between many types of published literatures. Based on analysis on the summary, our IQ dimension–attribute catalogue can be seen in Table 2. Each dimension has its own attributes which explains qualitative parameter for information quality.

Table 2. IQ Dimension-Attribute Catalogue

Dimension	Attribute	Code	Description
Accuracy	Correct	AC1	The degree of correctness form of information presentation to the user
	Free of error	AC2	Free of error during information production process
Objectivity	Unbiased	OB1	The data was obtained not because of assumptions or conjectures
Reliability	From good source	RE1	The data was obtained from correct source
Transferability	Free of network failure	TR1	Free of network failure during transfer process
	Sending media are good	TR2	Used media is effective and efficient
Content	Data are clear without ambiguity	CONT1	The data presented is clear and does not cause ambiguity
Consistency	Compatible with previous data	CONS1	In accordance with the data obtained. processed or stored before
	Presented in the same format	CONS2	Data elements are presented in the same format
Completeness	Complete	COM1	No missing data elements
	Include all necessary value	COM2	Includes all important information elements
Timeliness	Up to date	TI1	The degree of response to update
	Delivered on timely	TI2	The degree of all elements can be delivered on time
Security	Restricted appropriately	SE1	Information restrictions appropriately
	Secure	SE2	Security is maintained throughout the information production process

Input for this step is the scope or detail description of business process from the previous step. The detail of business process should be mapped to IP-MAP model [21]. From this model we get information and description on how the process of information production is performed. Through description from this model, we can understand what activity that is mapped to information production process (source, transfer, process) and what is the quality dimension requirement of each activity. In practice, we create questionnaire instrument based on the attribute of each dimension from the catalogue and relation to each activity. This instrument is used as a reference for IQ assessment process.

Step 3: Identify and estimate risk factor and risk profile.

In this step, risk factor identification is based on the catalogue of ISO/IEC 27005:2008. ISO 27001:2005 and a brief description in [16]. A risk is the probability of losses caused by threats, vulnerabilities and impacts [22]. Therefore, a risk is accumulation of probabilities associated with the risk itself. In this study, probabilities are calculated using subjective probabilities based on the knowledge and experience of the personnel involved in a process or system or experts. In Bayesian conditional probability, a prior opportunity represents a trust distribution reflecting the amount of initial trust of agents contributing to the hypothesis of an event [23]. In general, to calculate this probability value we refer to GB/T 20984-2007 [14, 24]. The detail of calculation of probability of risk factor and risk profile can be derived in the following steps.

1) Risk factor identification and estimation

a) Asset

Asset is defined as everything that has value to the organization and needs protection. In our conceptual model asset is expressed as variable Asset and Asset valuation can be divided in two variables: criticality and asset cost [25]. In our case, asset criticality is expressed on a qualitative scale following the standard given in [24]. The identification result of this asset which produce asset criticality level is expressed in the scale of 1 to 5.

b) Threat

On the conceptual model, a threat is denoted as variable T$_n$. A threat has the potential to harm assets such as information, processes, systems and even organizations. Threats can take the form of a natural or human origin and could be due to a deliberate or unintentional. According to [26], a vulnerability does not cause a risk if there are no threat to be exploited. Therefore, in our paper, we assume that a threat has dependent relationships with vulnerabilities. If the probability of vulnerability is increasing than it will be easier for threats to exploit. The probability of vulnerability indicates the degree of influence of vulnerability to the possible threat. Therefore, threat is a conditional probability of vulnerability. A threat occurs given vulnerabilities occurs. We use subjective Bayesian probability and expert perception as a prior probability. All of the above phenomena are described mathematically in the following:

$$P(T_{nt}|V_{nt}) = \frac{P(V_{nt}|T_{nt})P(T_{nt})}{\sum_{nt=1}^{NT} P(V_{nt}|T_{nt})P(T_{nt})} \tag{1}$$

$$P(RTL_{nt}) = P(T_{nt}|V_{nt}) \times \left(1 - P(LR_{nt})\right) \tag{2}$$

$$P(RTI_{nt}) = P(T_{nt}|V_{nt}) \times \left(1 - P(IR_{nt})\right) \tag{3}$$

where:

$P(T_{nt}|V_{nt})$: Probability of threats based on information from the probability of vulnerability (posterior).
$P(T_{nt})$: Probability of threat based on subject expert judgment (prior).
$P(V_{nt}|T_{nt})$: Probability that states the degree of vulnerability influence to threats.
$P(RTL_{nt})$: Probability of residue threat likelihood.
$P(RTI_{nt})$: Probability of residue threat impact.

after we obtain the threat probability, we could map the result to threat classification, where the qualitative classification consist of five level as in [24]. This quantitative classification is used to make it easier for classification process of threat probability.

c) Existing Control

Control as a way to lessen risk is divided into two types: (i) control that serves to reduce likelihood and (ii) control that serves to reduce impact. According to [16], likelihood reducers are dissuasive and preventive type of controls and the impact reducers are protective, palliative and recuperative types of control. Parameter α and β are the weight of each type of control. Weight ratio using α1:α2=1:2 and β1:β2:β3=1:2:2 [16]. The parameter $P(LR_{nt})$ is the effectiveness probability of likelihood reducer and $P(IR_{nt})$ is the effectiveness of impact reducer control.

$$P(LR_{nt}) = \frac{\alpha_1 \times P(DISS_{nt}) + \alpha_2 \times P(PREV_{nt})}{\alpha_1 + \alpha_2} \tag{4}$$

$$P(IR_{nt}) = \frac{\beta_1 \times P(PROT_{nt}) + \beta_2 \times P(PALL_{nt}) + \beta_3 \times P(RECU_{nt})}{\beta_1 + \beta_2 + \beta_3} \tag{5}$$

where:

$P(LR_{nt})$: Probability of likelihood reducer control effectiveness.
$P(IR_{nt})$: Probability of impact reducer control effectiveness.

d) Vulnerability

According to [26], incorrect or malfunctioning controls could become a vulnerability. Therefore, in this paper, the probability of vulnerability is calculated based on the value of the in-effective control of the associated vulnerability. One particular threat can exploit more than one vulnerability, while control is explicitly dedicated to overcoming such threat. So that the probability of vulnerability is calculated based on in-effective control of the threats that exploit relevant vulnerability. Therefore, eventhough parameter V_{nt} consists of $V_{1_{nt}}.\ldots.V_{nv_{nt}}$, it has only one probability value to represent the value of vulnerabilities in one relevant threat. We assume that in-effective probability of likelihood reduction does not affect each other (independent), and they are also independent to the in-effective probability of impact reduction, so that it is possible to use multiplication operation in (6).

$$P(V_{nt}) = \big(1 - P(LR_{nt})\big) \times \big(1 - P(IR_{nt})\big) \tag{6}$$

This vulnerability probability value is then mapped to vulnerability classification. We adopt the qualitative classification level in [24], which consist of five level. This quantitative classification is used to make classification process of vulnerability probability easier.

2) Probability of threat risk calculation

To calculate each likelihood and impact of each threat, we refer to [14]. Likelihood of threat risk (f_1) is a function of threat and vulnerability, while impact of threat risk (f_2) is a function of asset and vulnerability [14]. To calculate (f_1), we are using formula and weight (notation α and β) from [14] as in (7). Using (7), the result of threat risk likelihood calculation using two matrix dimensions can be seen in Table 3. The probability of likelihood is the result of f_1 divided by the maximum value of f_1 (25) where for threat level 5 the parameter α is 3, and for vulnerability level 5 then the parameter β is 2.

$$f_1 = \alpha t + \beta v \tag{7}$$

Table 3. Calculation of Threat Risk Likelihood Based on Two Matrix Dimension [14]

	f_1			V		
		1	2	3	4	5
T	1	3	4	5	10	12
	2	5	6	7	12	14
	3	7	8	9	14	16
	4	13	14	15	20	22
	5	16	17	18	23	25

for function (f_2), we perform some modification, since according to research result in [26]. vulnerability exploitation by threat could pose a risk. If there is no threat related to a certain vulnerability, then there would be no risk appear. Therefore, an impact is a function of threat, vulnerability and asset criticality. We assumed that threat and vulnerability have a mutually exclusive relationship as well as independent relationship between asset-threat and vulnerability, so that

$$f_2 = (\alpha t + \varphi v) \times \gamma a \tag{8}$$

The parameter α, φ and γ are the weight of each variable (t for threat level, v for vulnerability level and a for asset criticality level). In this study, we adopt the weight value from [14]. Based on our modification, we develop a new matrix of three dimensions for impact as shown in Table 4 which shows the matrix calculation result using formula (8). For illustration, using the weight as used in [14], the estimation result will be (i) when the threat level is 4 then parameter α is 3, (ii) when the vulnerability level is 2 then parameter φ is 2, and (iii) when the asset level is 5 then parameter γ is 2.5. Based on the estimate above and (8), f_2 is 200. The probability of impact will be the result of f_2 divided by the maximum value of f_2 (375) where the threat level is 5 for parameter α=3, the vulnerability level is 5 for φ=3, and the asset level is 5 for γ=2.5.

Following the description in [10], recoverability is defined as the system's ability to achieve acceptable limits or levels of operation after a risk event occurred. Therefore, to calculate recoverability, we assumed that recoverability is defined as the percentages (probability) of reduced threat (both of reduced likelihood threat and reduced impact threat) after controls are implemented. This probability value represents the organization's ability to reduce a certain threat. The parameter $P(RecL_{nt})$ is defined as recoverability related to the threat likelihood as in (9) and $P(RecI_{nt})$ defined as recoverability related to the threat impact as in (10).

Table 4. Calculation of Threat Risk Impact Based on Three Matrix Dimension

	f_2			A		
T	V	1	2	3	4	5
	1	4	8	30	40	50
	2	6	12	45	60	75
1	3	11	22	82.5	110	137.5
	4	14	28	105	140	175
	5	17	34	127.5	170	212.5
	1	6	12	45	60	75
	2	8	16	60	80	100
2	3	13	26	97.5	130	162.5
	4	16	32	120	160	200
	5	19	38	142.5	190	237.5
	1	8	16	60	80	100
	2	10	20	75	100	125
3	3	15	30	112.5	150	187.5
	4	18	36	135	180	225
	5	21	42	157.5	210	262.5
	1	14	28	105	140	175
	2	16	32	120	160	200
4	3	21	42	157.5	210	262.5
	4	24	48	180	240	300
	5	27	54	202.5	270	337.5
	1	17	34	127.5	170	212.5
	2	19	38	142.5	190	237.5
5	3	24	48	180	240	300
	4	27	54	202.5	270	337.5
	5	30	60	225	300	375

$$P(RecL_{nt}) = \frac{P(T_{nt}|V_{nt}) - P(RTL_{nt})}{P(T_{nt}|V_{nt})} \quad (9)$$

$$P(RecI_{nt}) = \frac{P(T_{nt}|V_{nt}) - P(RTI_{nt})}{P(T_{nt}|V_{nt})} \quad (10)$$

3) Probability of asset risk calculation

After probability value of each risk dimension (likelihood, impact and recoverability) for each threat is obtained, we can calculate the probability of each risk dimension related to certain asset. The likelihood and impact probability of an asset are joint probabilities of the threat risk relevant to the asset. For probability value of recoverability, we use the mean value probability of recoverability of each asset. We assumed that the threats on the same asset is mutually exclusive and independent. It means, threats in an asset may occur at the same time but the probability of those threat is independent each other.

$$P\left(\bigcup_{k=1}^{N} A_k\right) = \sum_{k=1}^{N} P(A_k) - \sum_{j=k}^{N} P\left(A_k \cap A_j\right) + .. + (-1)^{N+1} P(A_1 \cap .. \cap A_N) \quad (11)$$

notes

$P(A_k)$: Probability of likelihood/impact threat risk.

$P\ (A_k \cap A_j)$: Joint probability of likelihood/ impact/recoverability one threat risk to each other. Since threats in an asset are independent, then joint probability is calculated as $P(A_k) \times P(A_j)$.

Step 4: Calculating risk priority rank and calculating total impact.

1) Risk ranking estimation

Each dimension probability will be mapped to dimension classification of risk to represent risk matrix. The classification of each dimension is shown in Table 5, where we follow the classification described in [14]. The impact classification is created using the data in Table 4 and using k-means method [12] for classification. We can see that our proposed classification method can eliminate the subjectivity of classification by human decision maker. Meanwhile, the recoverability classification is calculated based on organization perception since it will be different from one organization to the other depends on their capability.

Table 5. Classification of Risk Matrix Dimension

Numeric	Likelihood Range		Impact Range	
1	0.01%	20.00%	0.01%	16.00%
2	20.01%	44.00%	16.01%	34.67%
3	44.01%	64.00%	34.68%	50.67%
4	64.01%	84.00%	50.68%	72.00%
5	84.01%	100.00%	72.01%	100.00%

In this paper, risk priority ranking is developed using extended risk matrix approach and Borda rank method. This method is more accurate than simple method of multiplying each level of risk matrix dimension as in [15]. Since the matrix dimension is extended by adding new dimension (recoverability). Borda rank method calculate four dimensions (likelihood, impact, likelihood recoverability and impact recoverability). In this paper, the objective of risks priority ranking is to inform the decision makers on the priority of risk and the list of assets who has the highest risk until lowest risk by considering the level of likelihood, impact, and recoverability. The highest rank means the asset has a highest level of likelihood and impact, but the lowest level of recoverability.

$$b_i = \sum_{k=1}^{m}(N - R_{ik}) \qquad (12)$$

where

N : Number of risk (asset).

k : Criteria of evaluation (L. I. RecL. RecI).

m : Number of k (m = 4).

$\mathrm{R_{ik}}$: Number risk which has greater than risk i on k criteria evaluation.

$\mathrm{b_i}$: Index of Borda for risk

2) Calculating total impact

In this paper, the calculation of total impact is limited to financial impact only. This impact is based on a technical impact for each dimension of information quality. We calculate the financial impact of each asset through gap percentages between ideal and actual information quality after risk occurs, then multiply the number by asset cost.

$$Tech_{nd_{na}} = \sum_{ni=1}^{NI}(P(I_{ni}) \times IQI_{nd}) \times \frac{1}{NI} \qquad (13)$$

$$F_{nd_{na}} = \frac{\left(IQI_{nd} - \left(IQD_{nd} - Tech_{nd_{na}}\right)\right)}{IQI_{nd}} \times AC \qquad (14)$$

where

$Tech_{nd_{na}}$: Technical impact of dimension.

$P(I_{ni})$: Probability of risk impact.

IQI_{nd} : Ideal value of IQ.

NI : Number of dimension that receive the impact.

$F_{nd_{na}}$: Financial impact of dimension.

IQA_{nd} : Actual value of IQ.

AC : Asset cost.

4. Real Case Illustration and Discussion

In this chapter, we will present a real case illustration of our proposed method in a government institution in Indonesia. Due to the nature of organization, we could not expose the name of the organization. We emphasize on their administration business process for the scope of implementation. We define and detail this scope into IP-MAP and identify each activity into information production phase (source, transfer and process). The summary of research results in [19] states that the dimensions which are important in government context are accuracy, transferability, completeness and security. Using IQ dimension–attribute catalogue in Table 2, we create several questionnaire instruments to find the existing and target of information quality. The result of this IQ assessment is shown in Table 6, where we can see that the lowest existing quality is in completeness dimension.

Table 6. Summary of Information Quality

Dimension	AC	TR	COM	TI	SE
Target	5.083	5.611	5.75	5.33	5.67
Existing	4.167	4.67	4.33	4.9167	4.89

To simplify the elaboration of the process, we will concentrate only on personnel asset (A7), the other assets will follow the same procedure. Based on identification step, there are 3 threats in asset A7, and we described this situation as in Figure 3 and Table 7 where implemented controls were related to maintain asset A7. To estimate the probability of risk factors (threats, control and vulnerabilities), we employ s (1), (2), (3), (4), (5), and (6), and to estimate the probability of risk profile of A7 (likelihood, impact, recoverability of likelihood and recoverability of impact) we use s (7), (8), (9) and (10), where the results can be seen in Table 8. To calculate probability of asset risk, we use (11) as joint probability of threats in an asset and the result is also shown in in Table 9 as a risk profile for asset A7. This procedure can be repeated for other assets, until finally we can find the complete risk profile of our case illustration institution as in Table 10. Our calculation result shows that first priority is in asset A2 which means that asset A2 has high likelihood, high impact but low recoverability.

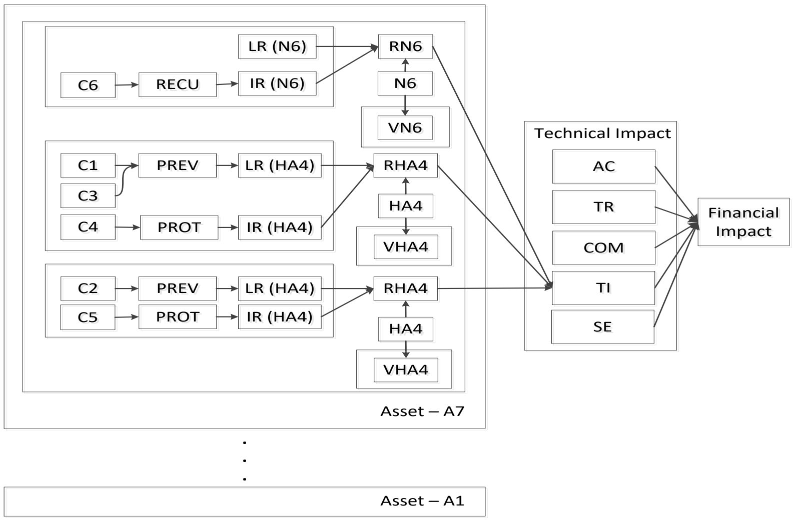

Figure 3. Implementation model

Table 7. Risk Factors Detail of A7

	Asset criticality	5	
	Asset cost	IDR 162000 (this asset cost is only for simulation)	
	Threats		Controls
Code	Description	Code	Description
N6	Storm	C6	Personal Liability Insurance
		C4	Determining the responsibility of termination and bonding managers
HA4	Organization deficiency	C1	Determining role and responsibility of information quality
		C3	Organization structure and job description
HA19	Lack of staff	C2	Personnel recruitment
		C5	Personnel rotation

Table 8. Threats-controls Estimation of A7

	Controls							Threat						
Threats Code	Code	Type	Effectiveness	Likelihood reducer	Impact reducer	Vulnerability		Unreduced Threat		Reduced likelihood of threat		Reduced impact of threat		
				$P(LR_{nt})$	$P(IR_{nt})$	$P(V_{nt})$	L	$P(T_{nt}\|V_{nt}$	L	$P(RTL_{nt})$	L	$P(RTI_{nt})$	L
N6	C6	RECU	62.30%	0.00%	24.92%	75.08%	4	20.08%	2	20.08%	2	15.08%	2
	C4	PROT	62.30%										
HA4	C1	PREV	62.30%	41.53%	12.46%	51.18%	3	52.65%	4	30.78%	3	46.09%	3
	C3	PREV											
HA19	C2	PREV	62.30%	41.53%	9.30%	53.03%	3	27.27%	3	15.95%	2	24.74%	2
	C5	PROT	46.50%										

Table 9. Summary of A7 Risk Profile

Code	f_1/25	f_2/375	Recoverability	
			$P(RecL_{nt})$	$P(RecI_{nt})$
N6	32.00%	40.00%	0.00%	24.92%
HA4	36.00%	40.00%	41.53%	12.46%
HA19	28.00%	33.33%	41.53%	9.30%

Table 10. Summary of Overall Assets Risk Profile

Asset Code	Likelihood		Impact		Recoverability				B	L
					Likelihood		Impact			
	P	L	P	L	P	L	P	L		
A1	87.58%	5	93.53%	5	34.22%	4	20.20%	4	24	3
A2	85.73%	5	90.95%	5	42.87%	4	15.64%	5	27	1
A3	77.05%	4	82.10%	5	48.41%	4	22.23%	4	21	4
A4	78.43%	4	83.08%	5	53.40%	3	17.77%	5	19	6
A5	54.52%	3	51.96%	4	32.86%	4	25.04%	4	13	7
A6	86.32%	5	87.95%	5	16.30%	5	20.08%	4	25	2
A7	68.67%	4	76.00%	4	27.69%	4	15.56%	5	19	5

We calculate each technical and financial impact of the threat using s (13) and (14) as shown in Table 11. From the table, we see that the difference between the existing condition after risk occurred and the target quality is 46%. It means the organization will be able to recover additional budget about IDR 73.762 (1:1000). The result provides us a way to analyze what dimensions are affected by a certain threat. For example, occurrence of threat N6 could affect staff's absence. In this case other staffs should cover his/her tasks and responsibilities, and it may cause accumulation of task. As a result, the tasks could not be delivered in timely manner. In our case illustration, all of threat in personnel asset unintentionally only affect timeliness dimension. For other assets the case might be different.

To evaluate the accuracy of risk priority ranking, we use mean absolute error through comparing actual rank with prediction rank for both cases without and with recoverability as illustrated in Table 12. As shown on the table, total error of risk rank without recoverability is higher than the one with recoverability. It means that the prediction with recoverability produces less error and increase the accuracy of risk rank. For the case where we add a new dimension, where we consider not only likelihood and impact but also recoverability, we implement Borda method. With this addition to the dimension, we can show that the Borda value is more diverse and decreasing the ambiguity of the priority risk ranking.

Table 11. Total Impact of A7

Code	$f_2/375$	Ideal quality	$Tech_{nd_{na}}$ (Timeliness)
N6	40.00%		2.13
HA4	40.00%	5.33	2.13
HA19	33.33%		1.78
Average			2.01
Actual after risk (4.9167–2.01)			2.90
Gap after risk (5.33–2.90)			46%
Financial impact of timeliness			IDR 73.762

Table 12. Summary of Comparing Risk Rank

Asset Code	Actual	Without recoverability				With recoverability					
	R	L	I	B	R	L	I	RecL	RecI	B	R
A1	2	5	5	14	2	5	5	4	4	24	3
A2	1	5	5	14	1	5	5	4	5	27	1
A3	4	5	5	14	5	4	5	4	4	21	4
A4	6	5	5	14	4	4	5	3	5	19	6
A5	7	4	4	3	7	3	4	4	4	13	7
A6	3	5	5	14	3	5	5	5	4	25	2
A7	5	4	5	9	6	4	4	4	5	19	5
Total error		4				2					

From simulation results, we can show that there are at least two benefits from our proposed method. First, the organization will be equipped with asset priority from the risk ranking where this ranking is created by considering not only the magnitude and level of risk likelihood and impact, but also the likelihood recoverability and impact recoverability as shown in Table 12. Second, the organization is provided with information on how much it would cost when the risk occurs. In our case illustration, we provide real data of organization, and calculate the financial impact of timeliness as presented in Table 11 amounted IDR 73.762. Using this value and the result of asset priority ranking with Borda method in Table 10, we can obtain two-dimensional quadrant relation of the seven assets as illustrated in Figure 4. Assets belong to the quadrant I should receive close attention and mitigation since this asset have a high cost and a high-risk rank. Meanwhile assets risk in quadrant IV could be accepted or in the last priority to mitigate.

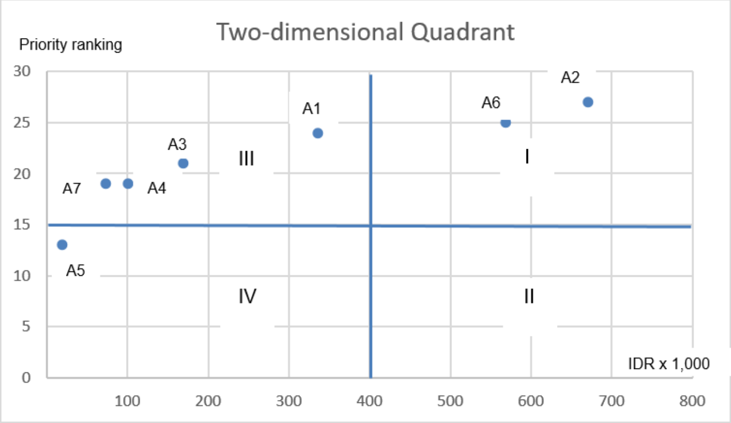

Figure 4. Two-dimensional quadrant relation of 7 assets

To compare the result of risk assessment, we evaluate it using mean absolute error and risk ties density shown in (15) and (16) below. We use mean absolute error in (15) to evaluate risk rank accuracy, whereas risk ties density in (16) is used to compare ambiguity of risk assessment result. In several cases, assessment result provide more than of one certain element (in our paper is IT assets) could occur in the same rank. It might make decision maker confused. With extended risk matrix approach instead of using only the likelihood and impact, by adding recoverability dimension the assessment result will be more complete and provide more consideration than only likelihood and impact. As the result of evaluation using mean absolute error and risk ties density, measured risk rank accuracy both of with and without recoverability dimension was 92.86% and 85.71%. Meanwhile measured risk ties density both of with and without recoverability dimension was 1.67 and 0.33.

$$Accuracy = 1 - \left(\frac{1}{n} \times \sum_{i=1}^{n} |f_i - y_i|\right) \times 100\% \quad (15)$$

$$d_t = \frac{\sum_{j=1}^{L} T_j}{L} \quad (16)$$

Where,
n : total of data
f_i : rank prediction of the system
y_i : rank prediction of the previous system
dt : risk ties density
Tj : number of risk ties in level j
L : total risk level

5. Conclusion

This paper proposed a new method to calculate the information quality risk assessment using extended risk matrix approach based on threat scenario dependency model. We include existing control effectiveness and IQ assessment result to calculate total impact. Through real implementation in a government institution, we have shown that the total impact reflects real condition more natural than the previously announced method. By considering existing control effectiveness in the calculation, we propose a new dimension of risk matrix called recoverability. In our real case illustration, by comparing actual ranking and prediction ranking using we can conclude that with our proposed method the accuracy is increasing and the risk ties on risk ranking is decreasing. It means that we can provide the organization with more accurate asset risk priority ranking where this ranking is created by considering not only the magnitude and level of risk likelihood and impact, but also the likelihood recoverability and impact recoverability. Moreover, we have shown that using out proposed method we provide the organization with information on how much it would cost when the risk occurs using simple but informative quadrant systems.

References

[1] Wang RY, Ziad M, Lee YW. *Data Quality*. New York. Boston. Dordrecht. London. Moscow: Kluwer *Academic Publishers* 2002.

[2] C Higson, D Waltho. Valuing Information as an Asset. *Sas Power To Know* 2010: 1–17.

[3] Borek A, Woodall P, *Towards a Process For Total Information Risk Management*. In: Proceedings of the 16th International Conference on Information Quality (ICIQ-2011). 2011: 477–491.

[4] Albarda, Supangkat SHAL. et al. Characteristics in Classification of Information Use (IU). *Int J Informatics Commun Technol*. 2014; 3(2): 180–185.

[5] O'Brien JA, Marakas GM. Management Information System. 2012. *Epub ahead of print* 2012.

[6] Laudon KC, Laudon JP. Management Information Systems Managing the Digital Firm. 1968. *Epub ahead of print* 1968.

[7] Borek A, Parlikad AK. Webb J. et al. *Total Information Risk Management*. 2014.

[8] Albarda. Information Characterization of Information Resource Services. Disertation. Bandung: *Postgraduate ITB*; 2014.

[9] Yan L, You Z, Jian L. *Marketing Outsourcing Risk Assessment in the Real Estate Based on Risk Matrix Model*. In: *I*nternational Conference on Information System for Crisi Response and Management. China. 2011: 134–138.

[10] Li ZP, Yee QMG, Tan PS, et al. An Extended Risk Matrix Approach for Supply Chain Risk Assessment. 2013; 1699–1704.

[11] Elmonstri M. Review of the strengths and weaknesses of risk matrices. 2014; 4: 49–57.

[12] He L, Chen Y, Lin LY. A Risk Matrix Approach Based on Clustering Algorithm. *J od Appl Sci* 2013; 13(20): 4188–4194.

[13] Zhu, Qichao, Kuang, et al. Risk Matrix Method and Its Application in the Field of Technical Project Risk Management. *Eingineering Sci* 2003; 5: 89–94.

[14] Xiangmo Z, Ming D, Shuai R, et al. Risk Assessment Model of Information Security for Transportation Industry System Based on Risk Matrix. 2014; 8(3): 1301–1306.

[15] Ni H, Chen A, Chen N. Some extensions on risk matrix approach. *Saf Sc.* 2010; 48(10): 1269–1278.

[16] Rahmad B, Supangkat SH, Sembiring J, et al. Threat Scenario Dependency-Based Model of Information Security Risk Analysis. 2010; 10(8): 93-102.

[17] ISO/IEC 27005:2008. *Information technology-Security-techniques-Information security risk management*. 2008.

[18] Albarda, Supangkat SH. Kuspriyanto. et al. Information Interchange Layer based on Classification of Information Use (IU). *TELKOMNIKA Telecommunication Computing Electronics and Control.* 2014; 12(2): 485–492.

[19] Nasution WS, Albarda. *Improvement of Business Process in order to Manage the Quality of Information*. In: International Conference on ICT for Smart Society (ICISS). 2013.

[20] Knight S, Burn J. Developing a Framework for Assessing Information Quality on the World Wide Web Introduction–The Big Picture What Is Information Quality ? 8.

[21] Shankaranarayanan G, Wang RY, Ziad M. IP-MAP : Representing the Manufacture of an Information Product. Proceedings of the 2000 Conference on Information Quality. 2000; 1–16.

[22] Alberts CJ. Common Elements of Risk.

[23] Joyce JM. The Development of Subjective Bayesian. *Sciencedirect*. 2009; 10: 1–62.

[24] GB/T 20984-2007. *Information security technology-Risk assessment specification for information security*. 2007.

[25] Sahinoglu M. Security Meter : *A Practical*. 2005; 18–24.

[26] ISO/IEC 27001:2005. INTERNATIONAL STANDARD ISO/IEC techniques—Information security. 2005.